W926

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-256004
(43)Date of publication of application : 21.09.2001

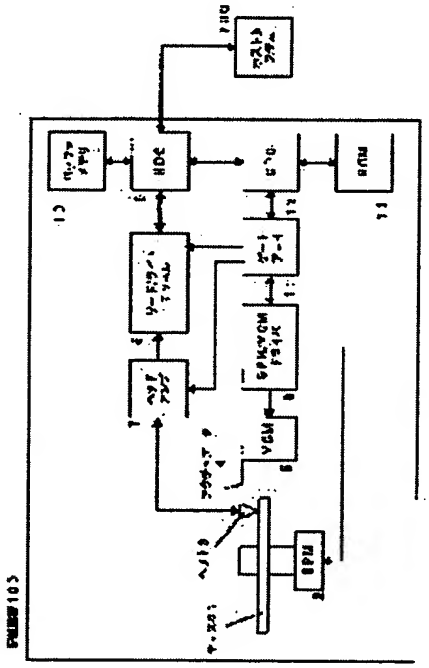
(51)Int.Cl. G06F 3/06
G06F 1/00
G06F 12/14
G11B 20/10

(21)Application number : 2000-069822
(22)Date of filing : 14.03.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : IGARI CHIKASHI

(54) INFORMATION STORAGE AND REPRODUCTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable restriction of access of a host system to user data in a storage device with respect to the storage device to be attachably/detachably connected with the host system.
SOLUTION: Authentication data for access control to be used in judgment of propriety of the access of the host system to the user data in the storage device are created in cooperation with the storage system and the host system and stored in both. And the storage device controls the access of the host system to the user data in the storage device based on the authentication data for access control stored in the host system and the authentication data for access control stored in the storage device in the case of judgment of the propriety of the access.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

W926

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－256004
（P2001－256004A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	3/06	３０４	Ｇ０６Ｆ 3/06	３０４Ｈ	５Ｂ０１７
	1/00	３７０	1/00	３７０Ｅ	５Ｂ０６５
	12/14	３２０	12/14	３２０Ａ	５Ｄ０４４
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ 20/10	Ｈ	

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）

(21)出願番号　特願2000－69822(P2000－69822)

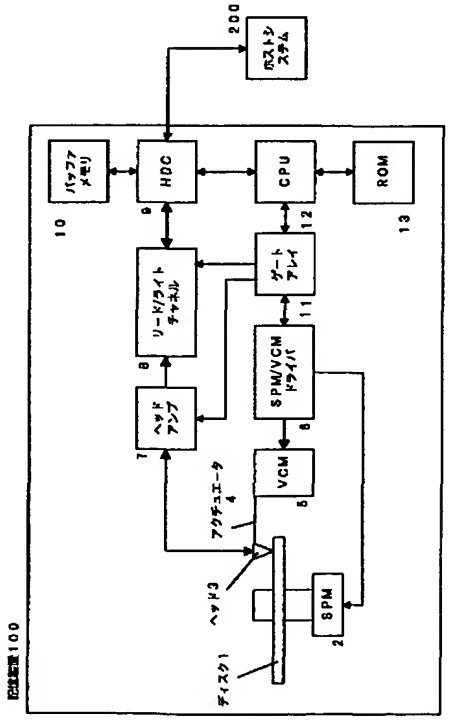
(22)出願日　平成12年３月14日(2000.3.14)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　猪狩　史
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

Ｆターム(参考)　5B017 AA03 BA05 BA09 CA06 CA14
5B065 BA01 PA06 PA14 ZA03
5D044 AB01 CC04 DE48 EF05 FG18
GK12 HL01

(54)【発明の名称】　情報記憶再生システム

(57)【要約】
【課題】　ホストシステムに着脱可能に接続される記憶装置において、記憶装置のユーザデータに対するホストシステムのアクセスを制限することを可能とする。
【解決手段】　記憶装置のユーザデータへのホストシステムのアクセス可否の判断において使用されるアクセス制御用認証データを、記憶装置とホストシステムとで共同して作成し、双方で記憶する。そして、アクセス可否の判断に際しては、記憶装置が、ホストシステムに記憶されているアクセス制御用認証データと記憶装置に記憶されているアクセス制御用認証データとに基づいて、記憶装置のユーザデータへのホストシステムのアクセス制御を行なう。



【特許請求の範囲】
【請求項１】　ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、
前記ホストシステム及び前記記憶装置は、前記ホストシステムが作成した認証データに基づいて前記記憶装置が作成した前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データ、又は、前記記憶装置が作成した認証データに基づいて前記ホストシステムが作成した前記アクセス制御用認証データを記憶する認証データ記憶手段をそれぞれ具備し、
前記記憶装置は、前記ホストシステムの前記認証データ記憶手段に記憶されたアクセス制御用認証データと、前記記憶装置の前記認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段を具備することを特徴とする情報記憶再生システム。
【請求項２】　前記ホストシステムは、当該ホストシステムの固有情報に基づき前記認証データ又は前記アクセス制御用認証データを作成することを特徴とする請求項１記載の情報記憶再生システム。
【請求項３】　前記記憶装置は、当該記憶装置の固有情報に基づき前記認証データ又は前記アクセス制御用認証データを作成することを特徴とする請求項１記載の情報記憶再生システム。
【請求項４】　ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、
前記ホストシステムは、
前記ホストシステム側の認証データであるホスト認証データを作成するホスト認証データ作成手段と、
前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データを記憶する第１の認証データ記憶手段とを具備し、
前記記憶装置は、
前記ホストシステムの前記ホスト認証データ作成手段により作成された前記ホスト認証データに基づいて前記アクセス制御用認証データを作成するアクセス制御用認証データ作成手段と、
前記アクセス制御用認証データ作成手段により作成された前記アクセス制御用認証データを記憶する第２の認証データ記憶手段と、
前記ホストシステムの前記第１の認証データ記憶手段に記憶されたアクセス制御用認証データと、前記第２の認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段とを具備することを特徴とする情報記憶再生システム。
【請求項５】　前記ホスト認証データ作成手段は、前記ホストシステムの固有情報に基づいて前記ホスト認証データを作成することを特徴とする請求項４記載の情報記憶再生システム。
【請求項６】　前記アクセス制御用認証データ作成手段は、前記ホストシステムの前記ホスト認証データ作成手段により作成された前記ホスト認証データと前記記憶装置の固有情報に基づいて前記アクセス制御用認証データを作成することを特徴とする請求項４記載の情報記憶再生システム。
【請求項７】　ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、
前記ホストシステムは、
前記記憶装置で作成される記憶装置認証データに基づいて前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データを作成するアクセス制御用認証データ作成手段と、
前記アクセス制御用認証データ作成手段により作成された前記アクセス制御用認証データを記憶する第１の認証データ記憶手段とを具備し、
前記記憶装置は、
前記記憶装置側の認証データである前記記憶装置認証データを作成する記憶装置認証データ作成手段と、
前記ホストシステムで作成された前記アクセス制御用認証データを記憶する第２の認証データ記憶手段と、
前記ホストシステムの前記第１の認証データ記憶手段に記憶されたアクセス制御用認証データと、前記第２の認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段とを具備することを特徴とする情報記憶再生システム。
【請求項８】　前記アクセス制御用認証データ作成手段は、前記記憶装置で作成される前記記憶装置認証データと前記ホストシステムの固有情報に基づいて前記アクセス制御用認証データを作成することを特徴とする請求項７記載の情報記憶再生システム。
【請求項９】　前記記憶装置認証データ作成手段は、前記記憶装置の固有情報に基づいて前記記憶装置認証データを作成することを特徴とする請求項７記載の情報記憶再生システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ユーザデータを記憶する記憶装置とこの記憶装置を着脱可能に接続してアクセスを行なうホストシステムとを有する情報記憶再生システムに関し、記憶装置側において、記憶装置にアクセスするホストシステムを特定のものに限定可能とする

情報記憶再生システムに関する。

【０００２】

【従来の技術】近年のハードディスクドライブ（ＨＤＤ）やＣＤ－ＲＯＭ等の記憶装置は、パーソナルコンピュータ等のホストシステムに、着脱可能な形態で使用できるようになっており、例えば、現在接続しているホストシステムから記憶装置を取り外して別のホストシステムに接続して使用することも可能である。

【０００３】このため、他のホストシステムが記憶装置をアクセスすることが可能であり、セキュリティ上の問題点があった。

【０００４】この問題点を解決するために、従来では、記憶装置に対するホストシステムからのアクセスを制限するためのセキュリティ方式が実現されている。この従来のセキュリティ方式は、ホストシステムが作成したパスワード（ホストシステムにおいてユーザが入力する）を予め記憶装置に記憶しておく。そして、ホストシステムから記憶装置へのアクセスが行なわれる際に、記憶装置において、ホストシステムから送信されるパスワード（ホストシステムにおいてユーザが入力する）が記憶装置に予め記憶されているものと一致するか否かを判断し、一致する場合にホストシステムに対してアクセスを許可するという方式をとっている。

【０００５】しかしこのセキュリティ方式では、ホストシステムが違っていてもホストシステムから記憶装置に送信されるパスワードが合っていれば、ホストシステムの違いに関係なく記憶装置はアクセスを許可することとなる。従って、記憶装置に予め記憶されているパスワードが他人に知られてしまうと、他人により別のホストシステムから不正にアクセスできてしまうといった課題がある。

【０００６】また、記録媒体に記録されたユーザデータへのアクセスを制御する技術としては、特開平１１－２２４４５６号に、光ディスクに対する情報処理装置のアクセスを制御する方法が記載されている。この従来技術では、情報処理装置に、光ディスクのＩＤとこの光ディスクにアクセスした際に発生する乱数を記憶し、一方、光ディスクに、上記したものと同様の乱数と情報処理装置のＩＤを記憶しておく。そして、情報処理装置が光ディスクに再度アクセスする時に、情報処理装置が、双方に記憶された３つの情報（光ディスクのＩＤ、乱数、情報処理装置のＩＤ）が全て一致するか否かを判断し、一致しない場合には光ディスクのアクセスを拒絶するようにしている。

【０００７】しかしこの方式は、アクセスの行なわれる側である光ディスクでは情報処理装置からのアクセスを制御できない。従って、例えば、上述した制御を無視して光ディスクにアクセスするよう不正に構成された情報処理装置が用いられ、光ディスクに不正にアクセスが行なわれた場合、光ディスク側ではその情報処理装置からの不正アクセスを抑制することができない。

【０００８】

【発明が解決しようとする課題】このように、従来のセキュリティ方式は、アクセスしようとするホストシステムの違いに関係なくパスワードが合っていれば記憶装置へのアクセスを許可していたため、他人が不正にパスワードを知り、そのパスワードを用いて他人の所有するホストシステムから不正にアクセスされる可能性があるが、その他人の所有するホストシステムからの不正アクセスを抑制することができないという課題があった。また、特開平１１－２２４４５６号に記載された方式では、アクセスする側の情報処理装置により不正アクセスが行なわれると、アクセスされる側の光ディスクではその不正アクセスを抑制できないという課題があった。

【０００９】本発明は上記の事情を考慮してなされたもので、記憶装置側において、当該記憶装置へのアクセスを特定のホストシステムにのみに制限することが可能な記憶装置及びホストシステムを有する情報記憶再生システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明の情報記憶再生システムは、ホストシステム及び記憶装置の各々の認証データ記憶手段に、ホストシステムが作成した認証データに基づいて前記記憶装置が作成した前記アクセス制御用認証データ、又は、記憶装置が作成した認証データに基づいてホストシステムが作成したアクセス制御用認証データを記憶する。そして、記憶装置の制御手段において、ホストシステムに記憶されたアクセス制御用認証データと、記憶手段に記憶されたアクセス制御用認証データとに基づいて、ホストシステムからのユーザデータへのアクセスを制御する。

【００１１】このように、ホストシステムと記憶装置との両方により作成したアクセス制御用認証データを用いることにより、記憶装置のユーザデータへのアクセスを特定のホストシステムにのみに制限することが可能となる。

【００１２】

【発明の実施の形態】（記憶装置の構成）先ず、本実施形態の記憶装置の構成を説明する。ここで、記憶装置は、例えば、ＨＤＤ、ＦＤＤ等の磁気ディスク装置や、ＤＶＤ、ＭＯ、ＣＤ－ＲＯＭ、ＭＤ等の光磁気ディスク装置、磁気テープ記憶装置、半導体メモリを用いた記憶装置等、ホストシステムに着脱可能に接続され使用されるものである。

【００１３】本実施形態では、記憶装置として、図１に示すように、ＨＤＤを想定している。ＨＤＤは、大別してユーザデータを記憶する記憶媒体としてのディスク１と、データのリード／ライト動作を実行するためのヘッド３と、リード／ライトデータの信号処理系と、制御系とから構成されている。ディスク１は、スピンドルモー

タ（ＳＰＭ）２により回転される。ヘッド３は、通常ではリードヘッドとライトヘッドとが同一スライダ上に実装されている。ヘッド３は、アクチュエータ４に搭載されて、ディスク１の半径方向に移動される。アクチュエータ４は、ボイスコイルモータ（ＶＣＭ）５を駆動源として、回転駆動するように構成されている。ＳＰＭ２及びＶＣＭ５は、後述するＣＰＵ１２の制御により、ＳＰＭ／ＶＣＭドライバ６から駆動電流を供給されて駆動する。ＳＰＭ／ＶＣＭドライバ６は、通常ではＣＰＵ１２からゲートアレイ１１を介してディジタルの制御値を入力し、当該制御値に応じて駆動電流を出力する。

【００１４】信号処理系は、ヘッドアンプ７及びリード／ライトチャネル８を有する。ヘッドアンプ７は、ヘッド３から読み出されたリード信号を増幅してリード／ライトチャネル８に送出する。また、ヘッドアンプ７は、リード／ライトチャネル８で処理されたライト信号（符号化された記録データ）を電流に変換してヘッド３に供給する。リード／ライトチャネル８は、エンコーダ及びデコーダを有し、ホストシステム２００からの書き込みデータをライト信号に変換し、且つ、ディスク１から読み出されたリード信号を元の書き込みデータに復号化するための各種信号処理を実行する。

【００１５】制御系は、ハードディスクコントローラ（ＨＤＣ）９と、ＣＰＵ１２と、ゲートアレイ１１とを有する。ＨＤＣ９は、ホストシステム２００との間でのデータ転送を制御するものであり、ホストシステム２００から入力されるデータを一次的にバッファメモリ１０に記憶させる等といった制御を行う。また、ＨＤＣ９は、図２に示すように、ＡＴＡコマンドの実行に必要な各種のレジスタを有する。ＣＰＵ１２は、ＲＯＭ１３に格納された制御プログラムに従って、後述する本実施形態の認証処理を実行する。ゲートアレイ１１は、主としてＣＰＵ１２の制御信号、及びリード／ライトチャンネル８からのサーボデータの入出力を制御するインターフェース制御回路に相当する。

（記憶装置側の認証処理）以下、記憶装置側の認証処理について説明する。

【００１６】図２に示すように、ＡＴＡインターフェース仕様のＨＤＣ９は、コマンドの実行処理に必要な各種のレジスタを有しているが、これら各種のレジスタの内、本実施形態の認証処理で使用されるレジスタは、コマンドレジスタ、セクタカウントレジスタ、エラーレジスタである。コマンドレジスタは、ホストシステム２００から送信される各種のコマンドを記憶する。セクタカウントレジスタは、ホストシステム２００から送信されるデータサイズ、及び、記憶装置１００から送信するデータサイズを示す情報を記憶する。エラーレジスタは、ホストシステム２００から送信されたコマンドに対する記憶装置１００の応答を示す情報を記憶する。

【００１７】以下、記憶装置側の認証処理を説明する。ここで、記憶装置１００における認証処理は、記憶装置１００に対して、ホストシステム２００側から電源投入が行なわれた後に実行されるものであり、ホストシステム２００から送信される各種のコマンドに応答する形態で実行される。

（記憶装置の第２次認証データの記憶有無の確認動作）図３は、ホストシステム２００に対して第２次認証データの記憶有無の応答を行なう記憶装置における処理を示すフローチャートである。

【００１８】第２次認証データは、記憶装置１００とホストシステム２００とが双方の固有情報を用いて共同で作成した認証データであり、記憶装置１００では、双方に記憶されている第２次認証データの比較を行うことで、ホストシステム２００に対してアクセス許可を行うか否かを判断する。また、ここでは、記憶装置１００とホストシステム２００のいずれも第２次認証データを記憶していない場合を想定して、以下に説明する。

【００１９】先ず、記憶装置１００に対して、ホストシステム２００から、記憶装置１００側に第２次認証データが記憶されているか否かを確認するため、認証データ確認コマンド（８Ｄｈ）が送信されると、記憶装置１００のＨＤＣ９では、そのコマンドレジスタに認証データ確認コマンド（８Ｄｈ）が書き込まれた状態となる。

【００２０】なお、ここでは認証コマンドを、（８Ｄｈ）という３文字の文字コードの組合わせを例として説明しているが、現在ＡＴＡコマンドに採用されている３文字の文字コードの組合わせ以外の組合せであれば何でもよい。また、以降の説明で、ホストシステム２００が送信する様々なコマンドを、所定の３文字の文字コードの組合わせで例示しているが、これは現在ＡＴＡコマンドで採用されている３文字の文字コードの組合わせ以外から例として示したものであり、これ以外でも現在ＡＴＡコマンドで採用されていないものであれば、どのような組合せでも良い。

【００２１】ＨＤＣ９のコマンドレジスタに認証データ確認コマンド（８Ｄｈ）が書き込まれた状態となるすると、記憶装置１００のＣＰＵ１２は、ＨＤＣ９のコマンドレジスタから認証データ確認コマンド（８Ｄｈ）を読出し（ステップＳ１）、コマンド内容を確認する（ステップＳ２）。コマンドが認証データ確認コマンド（８Ｄｈ）でない場合は、読み出された別のコマンドに対応した処理を行なうが（ステップＳ２のＮｏ）、この場合は認証データ確認コマンド（８Ｄｈ）であると確認されるため（ステップＳ２のＹｅｓ）、次いで、ＣＰＵ１２は、第２次認証データが記憶されているか否かを確認し、その確認結果をＨＤＣ９のエラーレジスタに書き込む（ステップＳ３）。ここで、第２次認証データは、ディスク１、ＲＯＭ１３（フラッシュＲＯＭ等の書き込みの行えるＲＯＭ）、ＣＰＵ１２内の図示しないＲＡＭのいずれに記憶しても構わないが、本実施形態では、例と

して、ＲＯＭ１３に記憶することとする。この場合、ＣＰＵ１２は、ステップＳ３において、ＲＯＭ１３に第２次認証データが記憶されているか否かを確認し、その確認結果をＨＤＣ９のエラーレジスタに書き込む。このＨＤＣ９のエラーレジスタには認識結果を示す情報として、第２次認証データが記憶されている場合は、（００ｈ）がセットされ、一方、記憶されていない場合は（０４ｈ）がセットされる。ここでは、記憶装置１００とホストシステム２００のいずれも第２次認証データを記憶していない場合を想定しているため、記憶装置１００のＲＯＭ１３には第２次認証データが記憶されておらず、ＣＰＵ１２は、第２次認証データが記憶されていないことを示す情報（０４ｈ）をエラーレジスタに書き込む。この時のＨＤＣ９の各レジスタの記憶内容を、図２に示している。ＣＰＵ１２は、確認結果をエラーレジスタに書き込むと、ホストシステム２００から送信された認証データ確認コマンド（８Ｄｈ）に対する処理を終了する。

【００２２】この結果、ホストシステム２００側では、ＨＤＣ９のエラーレジスタの記憶内容（０４ｈ）を読み出すことで、記憶装置１００に第２次認証データが記憶されていないことが認識されることとなる。その後、ホストシステム２００側では、ホストシステム２００自身に第２次認証データが記憶されているか否かを確認する処理が行われ、ホストシステム２００側に第２次認証データが記憶されていないと判断された場合は、ホストシステム２００側は、記憶装置１００との間に新たな接続関係を成立させることで記憶装置１００にアクセス可能にすべく、第２次認証データの作成を行なう処理が行われる。

【００２３】一方、ホストシステム２００側に第２次認証データが記憶されていると判断された場合には、ホストシステム２００側で、記憶装置１００へのアクセスを実行しない処理が行われることとなる。即ち、この場合、ホストシステム２００は、他の記憶装置に対してアクセスが許可された状態にある。本発明では、特定のホストシステムのアクセスを、特定の記憶装置にのみに限定するよう制御を行なうようにしている。このため、ホストシステム２００は、アクセスが許可されている他の記憶装置以外とはアクセスしないようにするため、今回アクセスしようとしている記憶装置１００へのアクセスを不許可とする。なお、ここで説明したホストシステム２００側の処理については、後に詳述する。

【００２４】ここでは、ホストシステム２００側も第２次認証データが記憶されていないので、ホストシステム２００側において、記憶装置１００との間に新たな接続関係を成立させ記憶装置１００にアクセスできるようにするため、第２次認証データを作成する処理がとられることとなる。このホストシステム２００側の第２次認証データ作成処理に対応して、記憶装置１００側では次に説明する第２次認証データ作成動作を行なう。

【００２５】（記憶装置側の第２次認証データの作成動作）記憶装置１００側の第２次認証データの作成動作について、図４に示すフローチャートを参照して説明する。

【００２６】ホストシステム２００が第２次認証データを作成する処理に移った場合、先ず、ホストシステム２００から記憶装置１００に対して、送信すべき第１次認証データのデータサイズを示す情報（０１ｈ）が送信され、続いて、第１次認証データ送信コマンド（８Ｆｈ）が送信される。ホストシステム２００から、第１次認証データのデータサイズを示す情報（０１ｈ）、及び、第１次認証データ送信コマンド（８Ｆｈ）が送信されると、図５のように、ＨＤＣ９のセクタカウントレジスタに（０１ｈ）、コマンドレジスタに（８Ｆｈ）がそれぞれ書き込まれる。ここでは、第１次認証データのデータサイズが５１２バイトであるため、その旨を示す情報として（０１ｈ）が送信される。

【００２７】ＣＰＵ１２では、ＨＤＣ９のコマンドレジスタから第１次認証データ送信コマンド（８Ｆｈ）を読出し（ステップＳ１１）、コマンド内容を確認する（ステップＳ１２）。コマンドが第１次認証データ送信コマンド（８Ｆｈ）でない場合は、読み出された別のコマンドに対応する処理行なうが（ステップＳ１２のＮｏ）、この場合は第１次認証データ送信コマンド（８Ｆｈ）であると確認されるため（ステップＳ１２のＹｅｓ）、ホストシステム１００から送信される第１次認証データを受信してバッファメモリ１０に記憶する。ＣＰＵ１２は、受信した第１次認証データにエラーがないことを確認すると、ＨＤＣ９のエラーレジスタの内容を（００ｈ）とし、エラーがない旨をホストシステム２００に知らせる（ステップＳ１３）。

【００２８】第１次認証データは、例えば、図６に示すように、ホストシステム２００において、当該ホストシステム２００の固有情報と、第１次認証データを作成する時の日時情報とに基づいて作成されたものである。この例では、ホストシステム２００の固有情報として、メーカ名（TOSHIBA）、機種名（Satellite2550X）、シリアル番号（99017796）を使用している。また、日時情報（1999-09-13，19:40:00）を使用している。第１次認証データは、５１２バイト（０００００ｈ～０１ＦＦｈ）で構成されるが、図６では、その中の０００００ｈ～０００２０ｈに上記した固有情報を示すデータが記述され、その後の０００３０ｈ～０１ＦＦｈにはデータの記述がなく全て「００ｈ」となっている。勿論、この０００３００ｈ～０１ＦＦｈにもデータが記述されるような更に長い第１次認証データを作成することも可能である。

【００２９】続いて、ＣＰＵ１２は、ホストシステム２００から送信された第１次認証データと記憶装置１００の固有情報から、第２次認証データを作成する（ステッ

プＳ１４）。ここで、記憶装置１００の固有情報は、ディスク１、ＲＯＭ１３、ＣＰＵ１２内の図示しないＲＡＭのいずれに記憶しても構わないが、本実施形態では、ＲＯＭ１３に記憶することとする。ＣＰＵ１２において作成される第２次認証データを、図７に示している。第２次認証データのデータサイズは５１２バイトであり、その前半の２５６バイト（００００ｈ～００ＦＦｈ）がホストシステム２００側で作成された第１次認証データであり、後半の２５６バイト（０１００ｈ～０１ＦＦｈ）に記憶装置２００の固有情報を付加した形式としている。記憶装置１００の固有情報は、メーカ名（TOSHIBA）、機種名（MK6411MAT）、シリアル番号（Z8G50891G）である。作成した第２次認証データは、一次的にＣＰＵ１２内の図示しないＲＡＭに記憶する。

【００３０】ＣＰＵ１２は、第２次認証データを作成すると、ホストシステム２００にエラー無く第２次認証データを作成したことを報知すべくＨＤＣ９のエラーレジスタに（０４ｈ）をセットし、ホストシステム２００から送信された第１次認証データ送信コマンド（８Ｆｈ）に対する処理を終了する。

（第２次認証データの送信）図８に示すフローチャートを参照して、記憶装置側の第２次認証データの送信動作を説明する。

【００３１】ホストシステム２００から第２次認証データの送信を要求すべく、記憶装置１００に対して、送信すべき第２次認証データのデータサイズ（５１２バイト）を示す情報（０１ｈ）が送信され、続いて、第２次認証データ受信コマンド（８１ｈ）が送信される。この時、図９のように、ＨＤＣ９のセクタカウントレジスタには（０１ｈ）、コマンドレジスタに第２次認証データ受信コマンド（８１ｈ）が書き込まれる。

【００３２】ＣＰＵ１２は、ＨＤＣ９のコマンドレジスタから第２次認証データ受信コマンド（８１ｈ）を読出し（ステップＳ２１）、コマンド内容を確認する（ステップＳ２２）。コマンドが第２次認証データ受信コマンド（８１ｈ）でない場合は、読み出された別のコマンドに対する処理を行なうが（ステップＳ２２のＮｏ）、この場合は第２次認証データ受信コマンド（８１ｈ）であると確認されるため（ステップＳ２２のＹｅｓ）、ＣＰＵ１２は、ホストシステム２００へ第２次認証データを送信することを報知するためにＨＤＣ９のエラーレジスタに（００ｈ）をセットした後、ＣＰＵ１２内の図示しないＲＡＭに記憶している第２次認証データをホストシステム２００へ送信し、また、ホストシステム２００への第２次認証データの送信を終了した後に、当該第２次認証データをＲＯＭ１３に記憶する（ステップＳ２３）。ステップＳ２３の処理を行うとＣＰＵ１２は、ホストシステム２００から送信された第２次認証データ受信コマンド（８１ｈ）に対する処理を終了する。

【００３３】この後、ホストシステム２００側では、記憶装置１００が送信した第２次認証データが記憶されることとなる。この結果、記憶装置１００とホストシステム２００との間で一対一の接続関係が成立される。従って、記憶装置１００側では、ステップＳ２３の処理を行うことにより、ＣＰＵ１２が、ディスク１のユーザデータへのアクセスを、ホストシステム２００に対して許可することとなる。一方、ホストシステム２００側は、記憶装置１００から第２次認証データが送信されることを受けて、記憶装置１００のディスク１のユーザデータへのアクセスが行える状態になったことを認識する。

【００３４】なお、記憶装置１００側において第２次認証データを記憶するタイミングを、ホストシステム２００へ第２次認証データの送信を終了した後としているのは、ホストシステム２００が第２次認証データを受取る前に誤ってホストシステム２００の電源が切断され記憶装置１００の方だけに第２次認証データが記憶されることを避けるためである。本発明では、記憶装置１００のみに第２次認証データが記憶されている場合は、記憶装置１００が、他のホストシステムにアクセスを許可している状態であることから、この他のホストシステム以外のホストシステムに対してはアクセスを不許可とするようにしている（この時の動作については後に詳述する）。このため、ホストシステム２００の電源切断により記憶装置１００側のみに第２次認証データが記憶されてしまうと、再度、記憶装置１００とホストシステム２００との間で認証処理を行う際に記憶装置１００へのアクセスが不許可となってしまうという不具合が生じるが、上記したように記憶装置１００での第２次認証データの記憶をホストシステム２００への第２次認証データ送信時とすることで、そのような不具合を回避することができる。

【００３５】また、上記したように設定した第２次認証データについて、記憶装置１００及びホストシステム２００から解除する方法は、従来のＡＴＡインターフェース仕様に記述されているセキュリティコマンドのパスワード解除の方法と同様である。即ち、ユーザにおいてホストシステム２００から第２次認証データの消去を指示可能なコマンドを設けておき、ユーザからのコマンド指示に応じて、記憶装置１００とホストシステム２００との双方で、第２次認証データの記憶を消去するようにする。第２次認証データを消去する処理は、記憶装置１００とホストシステム２００との双方とも同じであり、第２次認証データを記憶している記憶領域全体に対して（００ｈ）を書き込むことにより記憶内容を消去する。

（第２次認証データの比較動作）上述したように第２次認証データを作成した後は、ホストシステム２００側から記憶装置１００に対して当該記憶装置１００の電源が投入される際に、毎回、記憶装置１００側で、双方に記憶されている第２次認証データを比較し、ホストシステム２００に対してアクセスを許可するか否かを判断する

こととなる。この記憶装置１００の第２次認証データの比較動作について、図１０に示すフローチャートを参照して説明する。

【００３６】記憶装置１００に対して、ホストシステム２００から、送信すべき第２次認証データのデータサイズ（５１２バイト）を示す情報（０１ｈ）、及び、第２次認証データ送信コマンド（Ｆ４ｈ）が送信されると、図１１のように、記憶装置１００のＨＤＣ９のセクタカウントレジスタには（０１ｈ）、コマンドレジスタには第２次認証データ送信コマンド（Ｆ４ｈ）が書き込まれる。

【００３７】ＣＰＵ１２は、ＨＤＣ９のコマンドレジスタから第２次認証データ送信コマンド（Ｆ４ｈ）を読出し（ステップＳ３１）、コマンド内容を確認する（ステップＳ３２）。コマンドが第２次認証データ送信コマンド（Ｆ４ｈ）でない場合は、読み出された別のコマンドに対する処理を行なうが（ステップＳ３２のＮｏ）、この場合は第２次認証データ送信コマンド（Ｆ４ｈ）であると確認される（ステップＳ３２のＹｅｓ）。

【００３８】ＣＰＵ１２は、ホストシステム１００から送信される第２次認証データを受信してバッファメモリ１０に記憶する。（ステップＳ３３）。このとき、ＣＰＵ１２は、エラー無く第２次認証データを受信したことをホストシステム１００に報知すべく、ＨＤＣ９のエラーレジスタに（００ｈ）を書き込む。

【００３９】続いて、ＣＰＵ１２は、ホストシステム１００から送信された第２次認証データと記憶装置１００側で記憶している第２次認証データ（即ち、ＲＯＭ１３に記憶している第２次認証データ）とを比較する。ホストシステム２００側の第２次認証データと記憶装置１００側の第２次認証データとの比較の結果、一致していると判断した場合、ＣＰＵ１２は、ＨＤＣ９のエラーレジスタに（００ｈ）を書き込み、ホストシステム２００に対してディスク１のユーザデータへのアクセスを許可する旨報知する。一方、一致していない場合は、ＨＤＣ９のエラーレジスタに（０４ｈ）を書き込み、ホストシステム２００に対してディスク１のユーザデータへのアクセスを不許可とする旨を報知する（ステップＳ３４）。ＣＰＵ１２は、ＨＤＣ９のエラーレジスタに第２次認証データの比較結果を書き込むと、ホストシステム２００から送信された第２次認証データ送信コマンド（Ｆ４ｈ）に対する第２次認証データの比較処理を終了する。

【００４０】この後、ホストシステム２００側では、ＨＤＣ９のエラーレジスタの内容が確認されるが、エラーレジスタの内容が（００ｈ）の場合は、記憶装置１００が双方の第２次認証データが一致したと判断し、ディスク１のユーザデータへのアクセスを許可したことを認識し、以降のディスク１のユーザデータへのアクセスを行える状態が取られる。一方、エラーレジスタの内容が（０４ｈ）の場合は、ホストシステム２００側は、記憶装置１００が双方の第２次認証データが不一致としたと判断し、ディスク１のユーザデータへのアクセスを不許可としたことを認識し、以降の記憶装置１００のディスク１のユーザデータへのアクセスを行わない状態を取る。そして、ホストシステム２００側は、図示せぬ表示画面等において記憶装置１００へのアクセスが不許可となった旨をユーザに通知する。

（ホストシステム側の認証処理）次に、ホストシステム２００側の認証処理について、以下に説明する。

【００４１】ホストシステム２００は、パーソナルコンピュータや汎用コンピュータ等の各種のコンピュータである。ホストシステム２００は、図１２に示すように、ＡＴＡインターフェース回路２１、ＣＰＵ２２、ＲＯＭ２３、ＲＡＭ２４、ＲＴＣ２５等によって構成される。ＡＴＡインターフェース回路２１は、ＡＴＡ規格のインターフェースにて、記憶装置１００との間でのデータ転送を制御するものである。ＣＰＵ２２は、ホストシステム２００のメインの制御装置であり、ＲＯＭ２３や、ＲＡＭ２４に格納された制御プログラムに従って、認証処理を行う。また、ＲＯＭ２３は、ホストシステム２００の固有情報を記憶する。ＲＡＭ２４は、第２次認証データを記憶する。ＲＴＣ２５は、現在の日時情報を出力する。

【００４２】ホストシステム１００の認証処理を、図１３、１４を参照して説明する。

【００４３】先ず、ＣＰＵ２２は、記憶装置１００に第２次認証データが記憶されているか否かを問い合わせるため、ＡＴＡインターフェース回路２１を介して、記憶装置１００に認証データ確認コマンド（８Ｄｈ）を送信する（ステップＳ４１）。次いで、ＣＰＵ２２は、この認証データ確認コマンド（８Ｄｈ）に応答して記憶装置１００のＨＤＣ９のエラーレジスタに書き込まれた記憶内容を参照することで、記憶装置１００に第２次認証データが記憶されているか否かを判断する（ステップＳ４２）。

【００４４】記憶装置１００のＨＤＣ９のエラーレジスタの記憶内容が（００ｈ）である場合、ＣＰＵ２２は、記憶装置２００では第２次認証データが記憶されていないと判断し（ステップＳ４２のＮｏ）、次いで、ホストシステム１００自身に第２次認証データを記憶しているか否かを判断するため、ＲＡＭ２４に第２次認証データが記憶されているか否かを判断す（ステップＳ４３）。

【００４５】ホストシステム２００側にも第２次認証データが記憶されていない場合は（ステップＳ４３のＮｏ）、ホストシステム２００と記憶装置１００とが共に第２次認証データを記憶していないこととなるため、この場合、ホストシステム２００と記憶装置１００との間に新たな接続関係を成立させて記憶装置１００に対してアクセス許可を得るべく、以下に説明するステップＳ４４～ステップＳ４８の処理を行う。

【００４６】ＣＰＵ２２は、ＲＯＭ２３に記憶された固有情報とＲＴＣ２５から出力される日時情報とに基づいて第１次認証データ（図６）を作成する（ステップＳ４４）。そして、ＣＰＵ２２は、作成した第１次認証データを記憶装置１００に送信すべく、先ず、記憶装置１００に、送信すべき第１次認証データのデータサイズ（５１２バイト）を示す情報（０１ｈ）を送信し、続いて、第１次認証データ送信コマンド（８Ｆｈ）を送信する。第１次認証データ送信コマンド（８Ｆｈ）を送信した後、ＣＰＵ２２は、第１次認証データを記憶装置１００に送信する（ステップＳ４５）。

【００４７】次に、ＣＰＵ２２は、記憶装置１００に対して当該記憶装置１００で作成された第２次認証データを送信するように要求すべく、記憶装置１００に第２次認証データのデータサイズ（５１２バイト）を示す情報（０１ｈ）を送信し、続いて、第２次認証データ受信コマンド（８１ｈ）を送信する（ステップＳ４６）。記憶装置１００が、第２次認証データ受信コマンド（８１ｈ）の送信に応答して第２次認証データを送信することを報知すべくＨＤＣ９のエラーレジスタを（００ｈ）としたことを確認後、記憶装置１００から送信される第２次認証データを受信し、ＲＡＭ２４に記憶する（ステップＳ４７）。そして、ＣＰＵ２２は、記憶装置１００が、当該記憶装置１００のディスク１のユーザデータへのアクセスを許可したものと認識し、以降の記憶装置１００へのアクセスを行える状態とする（ステップＳ４８）。

【００４８】一方、ＣＰＵ２２は、ステップＳ４３の判断において、ＲＡＭ２４に第２次認証データが記憶されていると判断した場合は（ステップＳ４３のＹｅｓ）、ホストシステム２００側のみ第２次認証データが記憶されていることとなるため、記憶装置１００へのアクセスが不許可であると判断し、記憶装置１００へのアクセスを行わない状態とする（ステップＳ４９）。即ち、この場合、ホストシステム２００が他の記憶装置に対するアクセスが行なえる状態となっているため、ＣＰＵ２２は、アクセスが許可されている他の記憶装置以外の記憶装置にはアクセスを行なえないよう制御すべく、今回アクセスしようとしている記憶装置１００へのアクセスを不許可とする。

【００４９】次に、上記したステップＳ４２の判断で、記憶装置１００に第２次認証データが記憶されていると判断した場合を以下に説明する。

【００５０】ＣＰＵ２２は、ステップＳ４２において、記憶装置１００に第２次認証データが記憶されていると判断すると（ステップＳ４２のＹｅｓ）、次いで、ホストシステム２００自身に第２次認証データが記憶されているか否かを判断する（ステップＳ５０）。このステップＳ５０の処理は、上述したステップＳ４３と同様であり、ＣＰＵ２２がＲＡＭ２４に第２次認証データが記憶されているか否かを判断することで行う。このステップＳ５０の判断で、ホストシステム２００自身にも第２次認証データが記憶されていると判断した場合（ステップＳ５０のＹｅｓ）、ホストシステム２００と記憶装置１００共に、第２次認証データを記憶していることとなる。従って、この場合、ＣＰＵ２２は、ホストシステム２００の記憶している第２次認証データが記憶装置１００に記憶している第２次認証データと一致するか否かを確認すべく、送信すべき第２次認証データのデータサイズ（５１２バイト）を示す情報（０１ｈ）を送信し、続いて、第２次認証データ送信コマンド（Ｆ４ｈ）を記憶装置１００へ送信する。続いて、ＣＰＵ２２は、ＲＡＭ２４に記憶されている第２次認証データを記憶装置１００へ送信する（ステップＳ５１）。

【００５１】次に、ＣＰＵ２２は、送信した第２次認証データに対する記憶装置１００の比較結果を確認すべく当該記憶装置１００のＨＤＣ９のエラーレジスタの記憶内容を参照する（ステップＳ５２）。この結果、記憶装置１００のＨＤＣ９のエラーレジスタの内容が（００ｈ）の場合、ＣＰＵ２２は、記憶装置１００がアクセスを許可したと認識し、以降の記憶装置１００へのアクセスを行える状態とする（ステップＳ５３）。一方、エラーレジスタの内容が（０４ｈ）の場合は、ＣＰＵ２２は、記憶装置１００がアクセスを不許可としたことを認識する。そして、ＣＰＵ２２は、以降の記憶装置１００のディスク１のユーザデータへのアクセスを行わない状態とし、図示せぬ表示画面等において記憶装置１００へのアクセスが不許可となった旨をユーザに通知する（ステップＳ５４）。

【００５２】また、上述したステップＳ５０において、ホストシステム２００自身に第２次認証データを記憶していない場合（ステップＳ５０のＮｏ）は、記憶装置１００が第２次認証データを記憶しているのに対して、ホストシステム２００の方が第２次認証データを記憶していないこととなる。この場合、記憶装置２００は、他のホストシステムに対してアクセス許可を与えている状態であるため、アクセス許可が与えられている他のホストシステム以外は、記憶装置１００へのアクセスを不許可とする。従って、ＣＰＵ２２は、ステップＳ５４の処理へ移り、記憶装置１００へのアクセスは不許可とし、アクセス不許可の場合の処理を行う。

【００５３】また、このようにホストシステム２００側で認証処理を行った結果、記憶装置１００へのアクセスが許可とされた場合は（ステップＳ４８、若しくは、ステップＳ５３）、ホストシステム２００のＣＰＵ２２は、以降の処理において記憶装置１００へアクセスし、ユーザデータの読み書きを行うこととなる。

【００５４】以上説明したように、記憶装置１００とホストシステム２００との間で、互いの固有情報を用いて、共同して第２次認証データを作成し、このデータを

用いて互いの認証を行うようにしたため、記憶装置側においては、当該記憶装置へのアクセスを特定のホストシステムのみに限定するよう制御でき、また、ホストシステム側においては、特定の記憶装置のみに限定してアクセスを行うよう制御することが可能となる。

【００５５】なお、上述した本実施形態では、記憶装置１００やホストシステム２００の固有情報として、メーカ名、機種名、シリアル番号を用いているが、これに限らず、同一機種（若しくは類似機種を含めて）で全て異なるような数値（若しくは統計的に同一となる確立が非常に低い数値）を採用しても良い。更には、ユーザによって解析できないように固有情報を暗号化しても良い。

（第２の実施の形態）上述した実施形態では、ホストシステム２００側で第１次認証データを作成し記憶装置１００側で第２次認証データを作成するようにしているが、これとは逆に、記憶装置１００側で第１次認証データを作成しホストシステム２００側で第２次認証データを作成するようにしても良い。この第２の実施の形態について、以下に説明する。

【００５６】ここでは、先ず、ホストシステム２００側が、ホストシステム２００側及び記憶装置１００側に第２次認証データが記憶されているか否かを判断するが、この判断においてホストシステム２００側が、ホストシステム２００側にも記憶装置１００側にも第２次認証データが記憶されていないと判断した場合に、以下のような第２次認証データの作成動作を行なう。

【００５７】即ち、ホストシステム２００のＣＰＵ２２が、第１次認証データを作成するよう指示すべく記憶装置１００に対して第１次認証データ作成指示コマンドを送信する。記憶装置１００側のＣＰＵ１２では、その第１次認証データ作成指示コマンドを受けて、ＲＯＭ１３に記憶されている記憶装置１００の固有情報に基づいて第１次認証データを作成し、一次的にＣＰＵ１２内の図示しないＲＡＭに記憶する。

【００５８】次いで、ホストシステム２００側のＣＰＵ２２が、第１次認証データの送信を要求すべく記憶装置１００に対して第１次認証データ受信コマンドを送信する。記憶装置１００側のＣＰＵ１２では、その第１次認証データ受信コマンドを受けて、図示しないＣＰＵ１２内のＲＡＭに記憶している第１次認証データをホストシステム２００側へ送信する。

【００５９】ホストシステム２００側のＣＰＵ２２は、記憶装置１００側から第１次認証データを受信すると、この第１次認証データとＲＯＭ２３に記憶された固有情報とＲＴＣ２５から出力される日時情報とに基づいて第２次認証データを作成し、ＲＡＭ２４に記憶する。次いで、ホストシステム２００側のＣＰＵ２２は、作成した第２次認証データを送信すべく記憶装置１００に対して第２次認証データ送信コマンドを送信し、次いで、第２次認証データを送信する。

【００６０】記憶装置１００側のＣＰＵ１２では、第２次認証データ送信コマンドを受けると、この第２次認証データ送信コマンドに続いてホストシステム２００側から送信される第２次認証データを受信し、ＲＯＭ１３に記憶する。そして、第２次認証データをＲＯＭ１３に記憶した後、記憶装置１００側のＣＰＵ１２は、ＨＤＣ９のエラーレジスタに（０４ｈ）をセットすることで、ホストシステム２００にエラー無く第２次認証データを受信したことを報知する。

【００６１】ホストシステム２００側のＣＰＵ２２では、記憶装置１００側からエラー無く第２次認証データを受信した旨の報知を受けると、記憶装置１００側が、当該記憶装置１００のディスク１のユーザデータへのアクセスを許可したものと認識し、以降の記憶装置１００へのアクセスを行える状態とする。

【００６２】なお、第２次認証データの作成動作以外の処理動作、即ち、第２次認証データを作成するよりも前に、ホストシステム２００が当該ホストシステム２００及び記憶装置１００に第２次認証データが記憶されているか否かを判断する場合の処理動作や、第２次認証データを作成した後の記憶装置１００とホストシステム２００との間の第２次認証データの認証を行なう場合の処理動作等は、上述した第１の実施の形態の場合と同様である。

【００６３】

【発明の効果】以上詳述したように本発明によれば、記憶装置或いはホストシステムの一方で作成された認証データに基づいて他方がアクセス制御用の認証データを作成し、この認証データを用いてホストシステムのアクセス制御を行なうようにしたため、記憶装置側において、当該記憶装置へのアクセスを特定のホストシステムのみに限定するよう制御できる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る記憶装置の構成を示した図。

【図２】認証データ確認コマンド（８Ｄｈ）が書き込まれた時のＨＤＣ９の各種レジスタの内容を示す図。

【図３】記憶装置の第２次認証データの記憶有無の確認動作を示すフローチャート。

【図４】記憶装置の第２次認証データの作成動作を示すフローチャート。

【図５】第１次認証データ送信コマンド（８Ｆｈ）が書き込まれた時のＨＤＣ９の各種レジスタの内容を示す図。

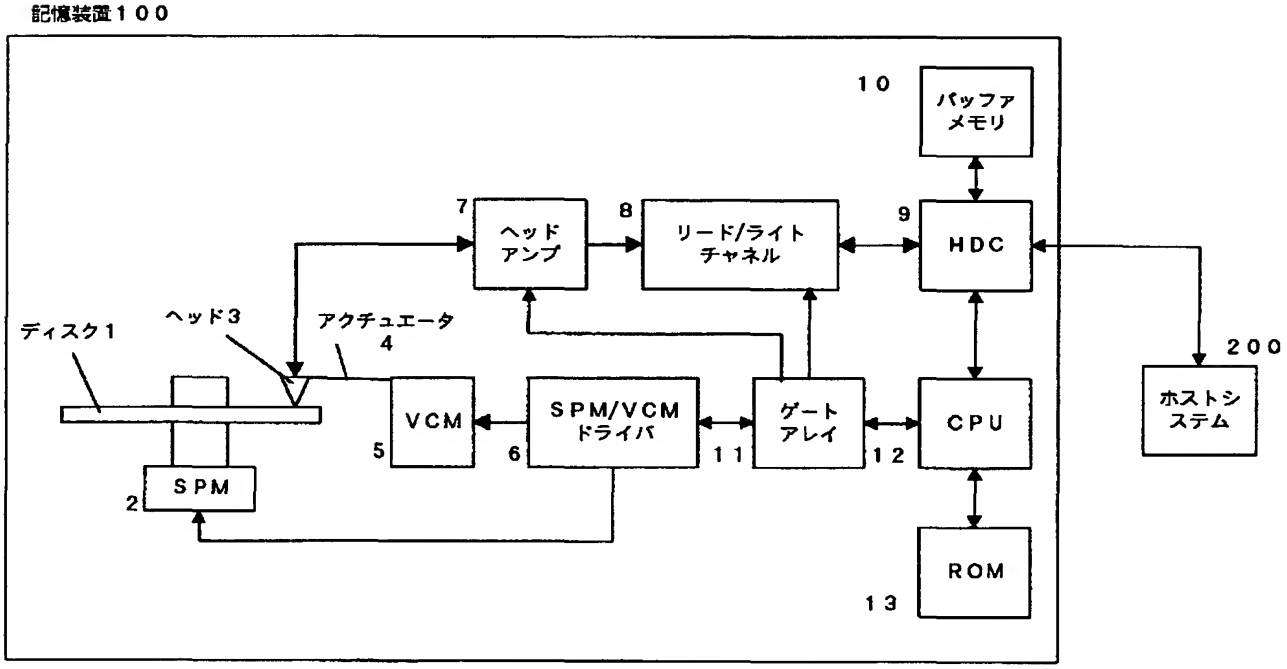
【図６】ホストシステムで作成される第１次認証データを示す図。

【図７】記憶装置で作成される第２次認証データを示す図。

【図８】記憶装置の第２次認証データの送信動作を示すフローチャート。

【図９】第２次認証データ受信コマンド（８１ｈ）が書き込まれた時のＨＤＣ９の各種レジスタの内容を示す図。
【図１０】記憶装置の第２次認証データの比較動作を示すフローチャート。
【図１１】第２次認証データ送信コマンド（Ｆ４ｈ）が書き込まれた時のＨＤＣ９の各種レジスタの内容を示す図。
【図１２】本発明の実施形態に係るホストシステムの構成を示す図。
【図１３】本発明の実施形態に係るホストシステムの認証処理を示すフローチャート。
【図１４】本発明の実施形態に係るホストシステムの認証処理を示すフローチャート。
【符号の説明】
１…ディスク
２…ＳＰＭ
３…ヘッド
４…アクチュエータ
５…ＶＣＭ
６…ＳＰＭ／ＶＣＭドライバ
７…ヘッドアンプ回路
８…リード／ライトチャネル
９…ＨＤＣ
１０…バッファメモリ
１１…ゲートアレイ回路
１２…ＣＰＵ（記憶装置側）
１３…ＲＯＭ（記憶装置側）
２１…ＡＴＡインターフェース回路
２２…ＣＰＵ（ホストシステム側）
２３…ＲＯＭ（ホストシステム側）
１００…記憶装置
２００…ホストシステム

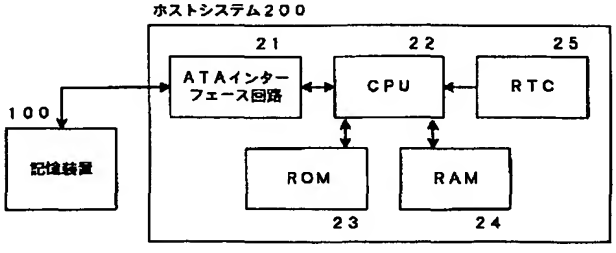
【図１】



【図６】

0000h	54h 4Fh 53h 48h 49h 42h 41h 2Ch 53h 61h 74h 65h 6Ch 6Ch 69h 74h "T" "O" "H" "S" "I" "B" "A" "," "S" "a" "t" "e" "l" "l" "i" "t"
0010h	65h 32h 35h 35h 30h 58h 2Ch 31h 39h 39h 39h 2Dh 30h 39h 2Dh 31h "e" "2" "5" "5" "0" "X" "," "1" "9" "9" "9" "-" "0" "9" "-" "1"
0020h	33h 2Ch 31h 39h 3Ah 34h 30h 3Ah 30h 30h 00h 00h 00h 00h 00h 00h "3" "," "1" "9" ":" "4" "0" ":" "0" "0"
0030h	00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h （0030h～01FFhまでのデータは全て「00h」）
01FFh	00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h

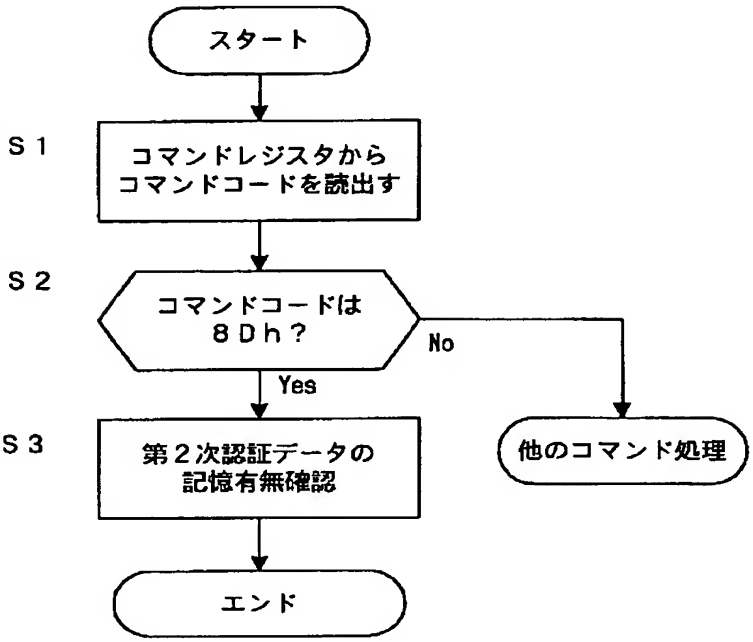
【図１２】



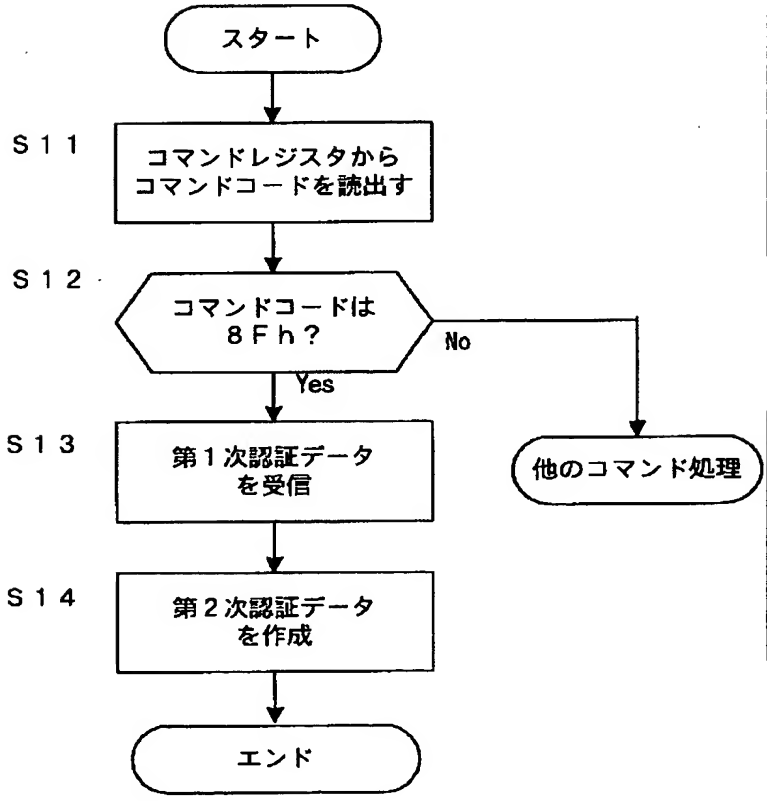
【図２】

レジスタ名	設定値
コマンドレジスタ	８Ｄｈ
セクタナンバレジスタ	（規定しない）
シリンダ・ロウレジスタ	（規定しない）
シリンダ・ハイレジスタ	（規定しない）
セクタカウントレジスタ	（規定しない）
ドライブ・ヘッドレジスタ	（規定しない）
フィーチャーレジスタ	（規定しない）
エラーレジスタ	０４ｈ

【図３】



【図４】



【図５】

レジスタ名	設定値
コマンドレジスタ	８Ｆｈ
セクタナンバレジスタ	（規定しない）
シリンダ・ロウレジスタ	（規定しない）
シリンダ・ハイレジスタ	（規定しない）
セクタカウントレジスタ	０１ｈ
ドライブ・ヘッドレジスタ	（規定しない）
フィーチャーレジスタ	（規定しない）
エラーレジスタ	００ｈ

【図９】

レジスタ名	設定値
コマンドレジスタ	８１ｈ
セクタナンバレジスタ	（規定しない）
シリンダ・ロウレジスタ	（規定しない）
シリンダ・ハイレジスタ	（規定しない）
セクタカウントレジスタ	０１ｈ
ドライブ・ヘッドレジスタ	（規定しない）
フィーチャーレジスタ	（規定しない）
エラーレジスタ	００ｈ

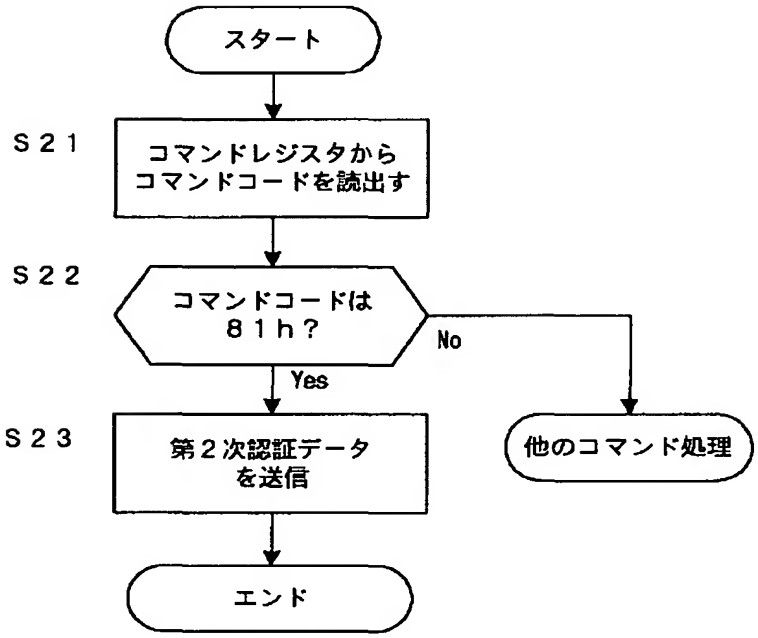
【図７】

```
0000h   54h 4Fh 53h 48h 49h 42h 41h 2Ch 53h 61h 74h 65h 6Ch 6Ch 69h 74h
        "T" "O" "H" "S" "I" "B"  "A" "," "S" "a"  "t"  "e" "l"  "l"  "i"  "t"
0010h   65h 32h 35h 35h 30h 58h 2Ch 31h 39h 39h 39h 2Dh 30h 39h 2Dh 31h
        "e"  "2" "5"  "5" "0"  "X" "," "1" "9" "9"  "9" "-"  "0" "9"  "-" "1"
0020h   33h 2Ch 31h 39h 3Ah 34h 30h 3Ah 30h 30h 00h 00h 00h 00h 00h 00h
        "3" "," "1" "9"  ":"  "4"  "0" "0"
0030h   00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
        (0030h～00FFhまでのデータは全て「00h」)

00FFh   00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h

0100h   54h 4Fh 53h 48h 49h 42h 41h 2Ch 4Dh 4Bh 36h 34h 31h 31h 4Dh 4Ah
        "T" "O" "H" "S" "I" "B"  "A" "," "M" "K"  "6"  "4" "1"  "1"  "M" "A"
0110h    54h 2Ch 5Ah 38h 47h 35h 30h 38h 39h 31h 47h   00h 00h 00h 00h 00h
        "T" "," "Z"  "8" "G"  "5" "0"  "8"  "9" "1" "G"
0120h   00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
        (0120h～01FFhまでのデータは全て「00h」)

01FFh   00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
```

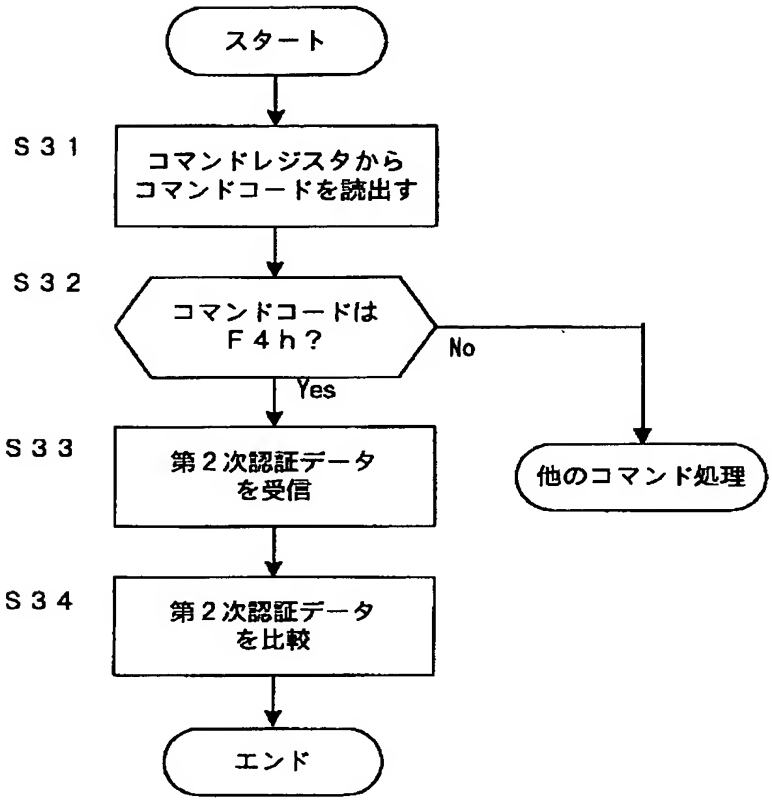
【図１１】

レジスタ名	設定値
コマンドレジスタ	Ｆ４ｈ
セクタナンバレジスタ	（規定しない）
シリンダ・ロウレジスタ	（規定しない）
シリンダ・ハイレジスタ	（規定しない）
セクタカウントレジスタ	０１ｈ
ドライブ・ヘッドレジスタ	（規定しない）
フィーチャーレジスタ	（規定しない）
エラーレジスタ	００ｈ

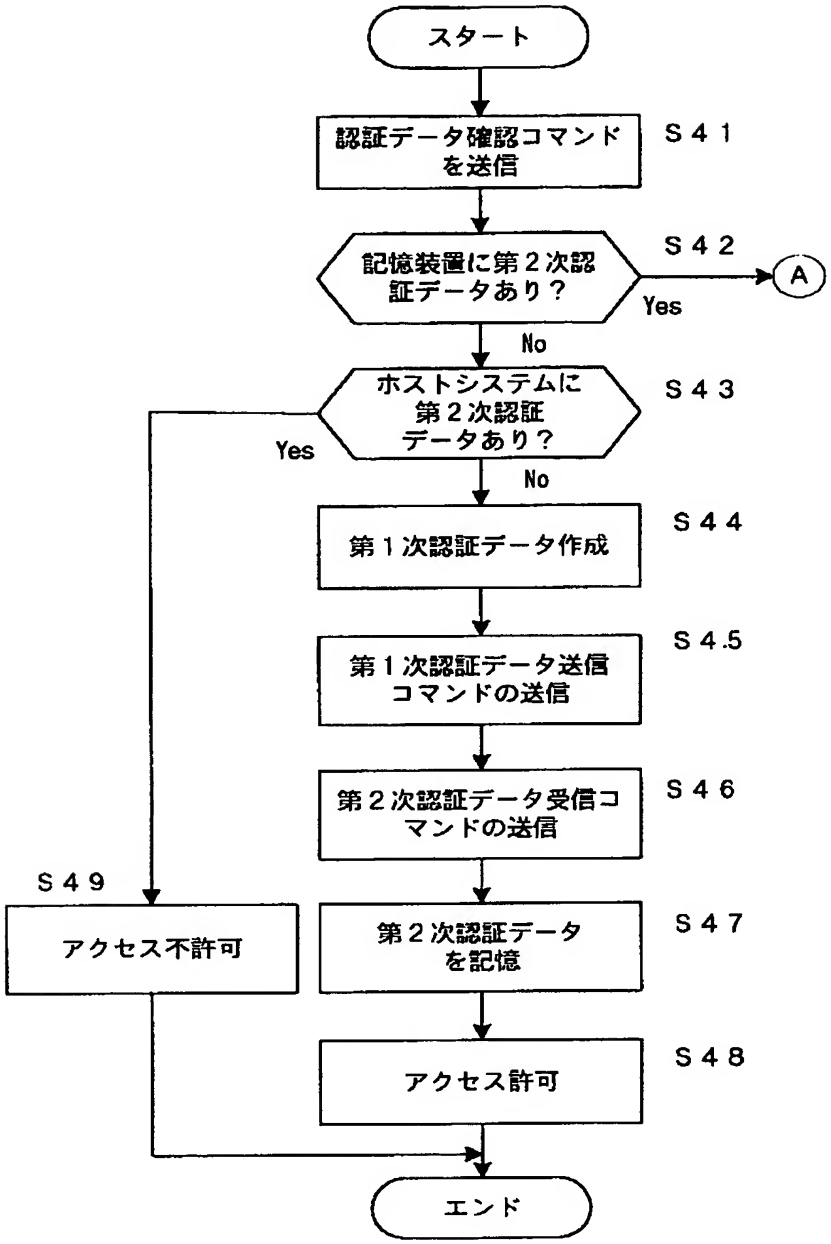
【図８】



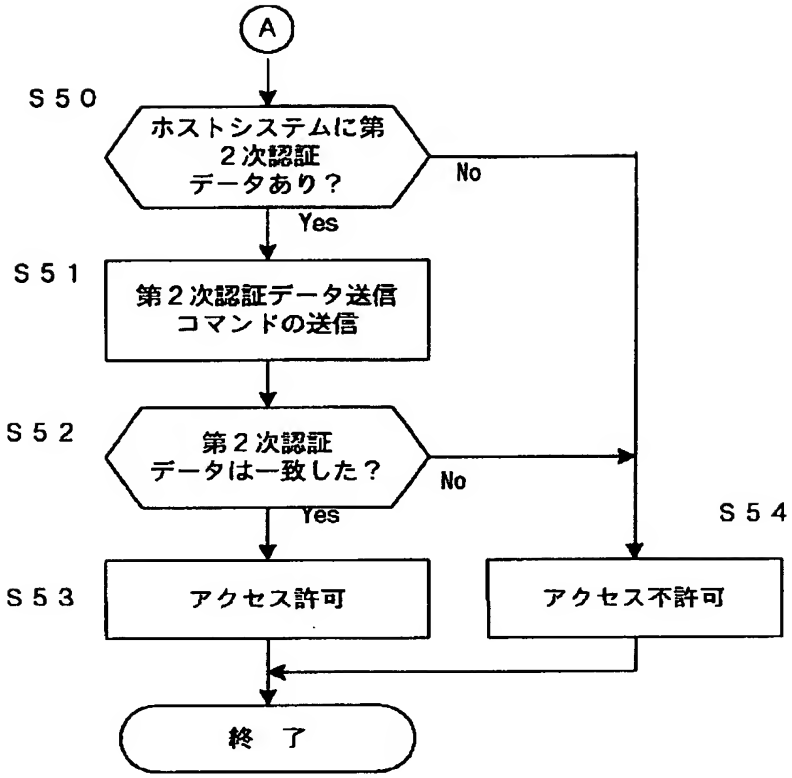
【図１０】


スタート
S３１
コマンドレジスタから
コマンドコードを読出す
S３２
コマンドコードは
Ｆ４ｈ？
No
Yes
S３３
第２次認証データ
を受信
他のコマンド処理
S３４
第２次認証データ
を比較
エンド

【図１３】


スタート
認証データ確認コマンドを送信
S４１
記憶装置に第２次認証データあり？
S４２
A
Yes
No
ホストシステムに第２次認証データあり？
S４３
Yes
No
第１次認証データ作成
S４４
第１次認証データ送信コマンドの送信
S４５
第２次認証データ受信コマンドの送信
S４６
S４９
アクセス不許可
第２次認証データを記憶
S４７
アクセス許可
S４８
エンド

【図１４】


A
S５０
ホストシステムに第２次認証データあり？
No
Yes
S５１
第２次認証データ送信コマンドの送信
S５２
第２次認証データは一致した？
No
Yes
S５４
S５３
アクセス許可
アクセス不許可
終　了